# EXHIBIT
# A

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

| | |
|---|---|
| SRI INTERNATIONAL, INC.,<br>a California corporation,<br><br>Plaintiff,<br><br>v.<br><br>INTERNET SECURITY SYSTEMS, INC.,<br>a Delaware corporation,<br>INTERNET SECURITY SYSTEMS, INC.,<br>a Georgia corporation, and<br>SYMANTEC CORPORATION,<br>a Delaware corporation,<br><br>Defendants. | Civil Action No. 04-1199 (SLR) |

## SYMANTEC CORPORATION'S INITIAL DISCLOSURES

Richard K. Herrmann (#405)
Morris, James, Hitchens & Williams LLP
222 Delaware Avenue, 10th Floor
P.O. Box 2306
Wilmington, DE 19899-2306
Telephone: (302) 888-6800
rherrmann@morrisjames.com

Counsel for Defendant
SYMANTEC CORPORATION

OF COUNSEL:

Lloyd R. Day, Jr. (*pro hac vice*)
Robert M. Galvin (*pro hac vice*)
Paul S. Grewal (*pro hac vice*)
Day Casebeer Madrid & Batchelder LLP
20300 Stevens Creek Blvd., Suite 400
Cupertino, CA 95014
Tel: (408) 873-0110
Fax: (408) 873-0220

Michael J. Schallop (*pro hac vice*)
Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
Tel: (408) 517-8000
Fax: (408) 517-8121

Dated: June 15, 2005

Defendant Symantec Corporation ("Symantec") provides these initial disclosures in compliance with Federal Rule of Civil Procedure 26(a) and the Court's June 3, 2005 Order. These initial disclosures are based on information reasonably available to Symantec at this time. Symantec reserves the right to supplement or amend these disclosures as warranted by further investigation.

## I.   INDIVIDUALS

The following individuals are likely to have discoverable information that Symantec may use to support its claims or defenses. Employees of Symantec should be contacted only through counsel for Symantec. To the extent known, contact information is provided for all other individuals.

| Name | Contact Information | Subject Matter |
|---|---|---|
| Adas, Victoria | Project Manager<br>Symantec<br>Cupertino, CA | ManHunt business issues, including Symantec's acquisition of Recourse |
| Almgren, Magnus | | Research relating to the alleged inventions claimed in the '338, '203, '212, and '615 patents |
| Anderson, Debra | | Research relating to the alleged inventions claimed in the '338, '203, '212, and '615 patents |
| Bachelor, Rod | Former Sr. Product Manager at Recourse Technologies<br><br>nCircle Network Security, Inc.<br>101 Second Street<br>Suite 400<br>San Francisco, CA 94105<br>(415) 625-5900 | ManHunt business issues at Recourse, including overall product direction, feature selection, and sales force training |

1

| Name | Contact Information | Subject Matter |
|---|---|---|
| Bagley, L. Mark | Technical Product Manager<br>Symantec<br>Redwood City, CA | ManHunt technical issues, including configuration and deployment |
| Bennett, Jeremy | Architect<br>Symantec<br>Redwood City, CA | ManHunt technical issues, including product design, development, deployment, and configuration |
| Bercow, Douglas | Director of Business Development<br>SRI International<br>333 Ravenswood Avenue<br>Menlo Park, CA 94025 | Efforts to commercialize the alleged inventions claimed in the '338, '203, '212, and '615 patents |
| Brobst, Jeff | VP Global Planning<br>Symantec<br>Cupertino, CA | Financial information regarding ManHunt |
| Castles, Wesley | Former VP Western Region Sales at Recourse Technologies<br><br>Symantec<br>Redwood City, CA | ManHunt business issues, including sales by Recourse |
| Cheung, Steven | SRI International<br>Room EL 227<br>333 Ravenswood Avenue<br>Menlo Park, CA 94025<br>(650) 859-5706 | Research relating to the alleged inventions claimed in the '338, '203, '212, and '615 patents |
| Choy, Benjamin | Director Licensing and Pricing<br>Symantec<br>Cupertino, CA | ManHunt business issues, including product pricing |
| Daniels-Sidon, Elizabeth | Manager Information Development<br>Symantec<br>Redwood City, CA | ManHunt technical issues, including product documentation |
| Feigenbaum, David L. | Fish & Richardson P.C.<br>225 Franklin Street<br>Boston, MA 02110<br>(617) 521-7817 | Prosecution of the '338 and '203 patents |

| Name | Contact Information | Subject Matter |
|---|---|---|
| Fitler, Bill | Former VP Engineering at Recourse Technologies<br><br>171 Frogsong Way<br>Watsonville, CA 95076 | ManHunt technical issues, including product engineering at Recourse |
| Fong, Martin W. | SRI International<br>Room EL 217<br>333 Ravenswood Avenue<br>Menlo Park, CA 94025<br>(650) 859-4251 | Research relating to the alleged inventions claimed in the '338, '203, '212, and '615 patents |
| Frivold, Thane | | Research relating to the alleged inventions claimed in the '338, '203, '212, and '615 patents |
| Geiger, Robert J. | Sr. Director Development<br>Symantec<br>Redwood City, CA | ManHunt technical issues, including product development |
| Gotta, Greg | VP Product Delivery<br>Symantec<br>Waltham, MA | ManHunt business issues |
| Gray, Wayne | Former VP Engineering at Recourse Technologies<br><br>(650) 625-0601 | Efforts to commercialize SRI's EMERALD project by AlertSoft, Inc.<br><br>ManHunt technical issues, including engineering, development, and quality assurance at Recourse |
| Greenberg, Robert A. | | Prosecution of the '338 patent |
| Gregory, Alexander | Technical Product Manager<br>Symantec<br>Redwood City, CA | ManHunt technical issues, including product features and functionality |
| Harrison, John H. | Product Manager<br>Symantec<br>Redwood City, CA | ManHunt technical issues, including product features and functionality |

| Name | Contact Information | Subject Matter |
|---|---|---|
| Hernacki, Brian | Architect<br>Symantec<br>Redwood City, CA | ManHunt technical issues, including product design and development |
| Herz, Rich | Manager of Contracts<br>SRI International<br>333 Ravenswood Avenue<br>Menlo Park, CA 94025 | Government contracts regarding technology relating to the alleged inventions claimed in the '338, '203, '212, and '615 patents |
| Huerta, Frank | Former CEO at Recourse Technologies | ManHunt business issues at Recourse |
| Janczura, Mark | Manager Development<br>Symantec<br>Redwood City, CA | ManHunt technical issues, including design and development |
| Javitz, Hal | Principal Scientist<br>SRI International<br>333 Ravenswood Avenue<br>Menlo Park, CA 94025 | Research relating to the alleged inventions claimed in the '338, '203, '212, and '615 patents |
| Jawetz, Michael | Principal Systems Engineer<br>Symantec<br>Redwood City, CA | ManHunt technical issues, including deployment and configuration |
| Khouri, John | SRI International<br>Room EL 223<br>333 Ravenswood Avenue<br>Menlo Park, CA 94025<br>(650) 859-4247 | Research relating to the alleged inventions claimed in the '338, '203, '212, and '615 patents |
| Kost, Fred | Former VP Marketing and VP Engineering at Recourse Technologies<br><br>Blue Lane Technologies, Inc.<br>2901 Tasman Drive<br>Suite 113<br>Santa Clara, CA 95054<br>(408) 492-1001 | ManHunt technical issues, including engineering at Recourse<br><br>ManHunt business issues, including marketing at Recourse |

| Name | Contact Information | Subject Matter |
|------|-------------------|----------------|
| Kozik, Kenneth F. | Fish & Richardson P.C.<br>225 Franklin Street<br>Boston, MA 02110<br>(617) 521-7837 | Prosecution of the '338, 203, and '615 patents |
| Kumar, Sandeep | Director Product Management<br>Symantec<br>Redwood City, CA | ManHunt technical issues, including product features and functionality<br><br>ManHunt business issues, including marketing |
| Lincoln, Patrick | Lab Director<br>SRI International<br>333 Ravenswood Avenue<br>Menlo Park, CA 94025 | Efforts to commercialize the alleged inventions claimed in the '338, '203, '212, and '615 patents |
| Lindgvist, Ulf | SRI International<br>Room EL 229<br>333 Ravenswood Avenue<br>Menlo Park, CA 94025<br>(650) 859-2351 | Research relating to the alleged inventions claimed in the '338, '203, '212, and '615 patents |
| Linne, Donna | Contracts Manager<br>SRI International<br>333 Ravenswood Avenue<br>Menlo Park, CA 94025 | Government contracts regarding technology relating to the alleged inventions claimed in the '338, '203, '212, and '615 patents |
| Lockwood, Mark | Technical Product Manager<br>Symantec<br>Redwood City, CA | ManHunt technical issues, including product features and functionality<br><br>Manhunt business issues, including marketing |
| Luk, William | Manager Development<br>Symantec<br>Redwood City, CA | ManHunt technical issues, including product design and development |
| Lyle, Mike | Former CTO at Recourse Technologies | ManHunt technical issues, including product design and development at Recourse |

5

| Name | Contact Information | Subject Matter |
|------|-------------------|----------------|
| Moran, Douglas B. | Former VP Research and Development at Recourse Technologies<br><br>790 Matadero Ave<br>Palo Alto, CA 94306<br>(650) 856-3302 | ManHunt technical issues, including development and testing at Recourse<br><br>ManHunt business issues, including marketing at Recourse |
| Neumann, Peter G. | SRI International<br>Room EL 243<br>333 Ravenswood Avenue<br>Menlo Park, CA 94025<br>(650) 859-2375 | Research relating to the alleged inventions claimed in the '338, '203, '212, and '615 patents<br><br>Efforts to commercialize the alleged inventions claimed in the '338, '203, '212, and '615 patents |
| Nitz, Kenneth | SRI International<br>Room EL 231<br>333 Ravenswood Avenue<br>Menlo Park, CA 94025<br>(650) 859-2804 | Research relating to the alleged inventions claimed in the '338, '203, '212, and '615 patents |
| Porras, Phillip A. | SRI International<br>Room EL 219<br>333 Ravenswood Avenue<br>Menlo Park, CA 94025<br>(650) 859-3232 | Research relating to the alleged inventions claimed in the '338, '203, '212, and '615 patents<br><br>Prosecution of the '338, '203, '212, and '615 patents<br><br>Efforts to commercialize the alleged inventions claimed in the '338, '203, '212, and '615 patents |
| Salem, Enrique T. | Sr. VP Gateway Solutions<br>Symantec<br>San Francisco, CA | ManHunt business issues |
| Shirtong, Frank | Manager Development<br>Symantec<br>Redwood City, CA | ManHunt technical issues, including product design and development |

| Name | Contact Information | Subject Matter |
|---|---|---|
| Skinner, Keith | SRI International<br>Room EL 225<br>333 Ravenswood Avenue<br>Menlo Park, CA 94025<br>(650) 859-3612 | Research relating to the alleged inventions claimed in the '338, '203, '212, and '615 patents |
| Smith, Sandy | SRI International<br>Room EL 231<br>333 Ravenswood Avenue<br>Menlo Park, CA 94025<br>(650) 859-2200 | Research relating to the alleged inventions claimed in the '338, '203, '212, and '615 patents |
| Standenraus, John | Former co-founder of AlertSoft<br><br>Symantec<br>Cupertino, CA | Efforts to commercialize SRI's EMERALD project by AlertSoft, Inc. |
| Stavridou-Coleman, Victoria | Former Director of System Design Laboratory at SRI International<br><br>Intel Corporation<br>2200 Mission College Blvd.<br>Santa Clara, CA 95052 | Research relating to the alleged inventions claimed in the '338, '203, '212, and '615 patents |
| Stringer-Calvert, David | Director of IP<br>SRI International<br>333 Ravenswood Avenue<br>Menlo Park, CA 94025 | Efforts to commercialize the alleged inventions claimed in the '338, '203, '212, and '615 patents |
| Thaler, Joshua | Former Dir. Release Engineering, Quality Assurance, and Support Engineering at Recourse Technologies<br><br>Proofpoint, Inc.<br>10201 Torre Avenue<br>Suite 100<br>Cupertino, CA 95014<br>(408) 850-4067 | ManHunt technical issues, including quality assurance testing and support engineering at Recourse |
| Tong, Kin-Wah | Moser, Patterson & Sheridan, LLP<br>595 Shrewsbury Avenue, Suite 100<br>Shrewsbury, NJ 07702<br>(732) 530-9404 | Prosecution of the '212 and '615 patents |

| Name | Contact Information | Subject Matter |
|---|---|---|
| Valdez, Alfonso | SRI International<br>Room EL 221<br>333 Ravenswood Avenue<br>Menlo Park, CA 94025<br>(650) 859-4976 | Research relating to the alleged inventions claimed in the '338, '203, '212, and '615 patents<br><br>Prosecution of the '338, '203, '212, and '615 patents<br><br>Efforts to commercialize the alleged inventions claimed in the '338, '203, '212, and '615 patents |
| Weiner, Steven | Former in-house IP Counsel of SRI International<br><br>Davis Polk & Wardwell<br>1600 El Camino Real<br>Menlo Park, CA 94025 | |
| Wheeler, Patrick | Product Manager<br>Symantec<br>Redwood City, CA | ManHunt technical issues, including product features and functionality |
| Williams, Cynthia | VP Revenue Accounting<br>Symantec<br>Cupertino, CA | Financial information regarding ManHunt |
| Wood, William | Sr. Manager SQA Engineering<br>Symantec<br>Redwood City, CA | ManHunt technical issues, including quality assurance testing |

## II.    DOCUMENTS[1]

The following categories of documents believed to be in the possession, custody, or control of Symantec may be used to support Symantec's claims or defenses.

1.    U.S. Patent Nos. 6,321,338, 6,484,203, 6,708,212, and 6,711,615;

---

[1] Identification of a category of documents that Symantec may use to support its claims or defenses does not constitute a waiver of any claims under the attorney-client privilege or the attorney work-product doctrines.

2.    Patent prosecution files for U.S. Patent Nos. 6,321,338, 6,484,203, 6,708,212, and 6,711,615, including cited art;

3.    Publications that are prior art to U.S. Patent Nos. 6,321,338, 6,484,203, 6,708,212, and 6,711,615;

4.    Documents regarding SRI's EMERALD project;

5.    Communications between Symantec and SRI regarding ManHunt and/or U.S. Patent Nos. 6,321,338, 6,484,203, 6,708,212, and 6,711,615;

6.    ManHunt technical information, including source code; and

7.    ManHunt marketing, licensing, and/or sales information.

These documents are located primarily at Symantec's offices in Cupertino and Redwood City, California.

## III.    EXPERT WITNESSES

Symantec has not yet identified persons whom it intends to have testify as experts.

## IV.    INSURANCE AGREEMENTS

Symantec is not aware of any insurance agreements that pertain to issues identified in the pleadings in this action.

## V.    DAMAGES

Symantec is not currently seeking to recover damages beyond its costs and attorneys' fees.

Dated: June 15, 2005

By: _____
Richard K. Herrmann (#405)
Morris, James, Hitchens & Williams LLP
222 Delaware Avenue, 10th Floor
P.O. Box 2306
Wilmington, DE 19899-2306
Telephone: (302) 888-6800
rherrmann@morrisjames.com

Counsel for Defendant
Symantec Corporation

OF COUNSEL:

Lloyd R. Day, Jr. (*pro hac vice*)
Robert M. Galvin (*pro hac vice*)
Paul S. Grewal (*pro hac vice*)
Day Casebeer Madrid & Batchelder LLP
20300 Stevens Creek Blvd., Suite 400
Cupertino, CA 95014
Tel: (408) 873-0110
Fax: (408) 873-0220

Michael J. Schallop (*pro hac vice*)
Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
Tel: (408) 517-8000
Fax: (408) 517-8121

# EXHIBIT
# B

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a California
Corporation,

        Plaintiff,

v.

INTERNET SECURITY SYSTEMS, INC.,
a Delaware corporation, INTERNET
SECURITY SYSTEMS, INC., a Georgia
corporation, and SYMANTEC
CORPORATION, a Delaware corporation,

        Defendants.

Case No. 04-1199-SLR

**PLAINTIFF SRI INTERNATIONAL, INC.'S FIRST SET OF
INTERROGATORIES TO DEFENDANT SYMANTEC CORPORATION
[NOS. 1–13]**

Pursuant to Rules 26 and 33 of the Federal Rules of Civil Procedure, Plaintiff SRI International, Inc. hereby requests Defendant Symantec Corporation to answer in writing and under oath the following Interrogatories within thirty (30) days after service.

## DEFINITIONS AND INSTRUCTIONS

A.  "SRI" means SRI International, Inc., including its officers, directors, employees, agents, and attorneys.

B.  "Symantec," "Defendant," "you," or "your" means Symantec Corporation, including its past and present officers, directors, employees, consultants, agents, and attorneys and others acting or purporting to act on its behalf, and including their predecessors, subsidiaries, parents, and affiliates.

C.  The phrase the "'615 patent" means U.S. Patent No. 6,711,615.

D.  The phrase the "'203 patent" means U.S. Patent No. 6,484,203.

E.  The phrase the "'338 patent" means U.S. Patent No. 6,321,338.

F.  The phrase the "'212 patent" means U.S. Patent No. 6,708,212.

G.    The phrase the "'874 patent" means U.S. Patent No. 6,704,874.

H.    The phrase "Patents-in-Suit" means the '615, '203, '338, '212, and '874 Patents.

I.    The word "Document" is used herein in its broadest sense to include everything that is contemplated by Rule 26 and Rule 34 of the Federal Rules of Civil Procedure, including Documents stored in hard copy or electronic form. Electronic Documents include electronic mail, computer source code, object code, and microcode, and Documents stored on any media accessible by electronic means. A comment or notation appearing on any "Document" and not a part of the original text is to be considered a separate "Document".

J.    "Thing" means any tangible object other than a Document.

K.    "Person" or "Persons" include not only natural individuals, but also, without limitation, firms, partnerships, associations, corporations, and other legal entities, and divisions, departments, or other units thereof.

L.    These "Interrogatories" shall mean the instant document, i.e., Plaintiff SRI International, Inc.'s First Set of Interrogatories to Defendant Symantec Corporation [Nos. 1–13].

M.    "Including" shall mean "including but not limited to."

N.    The terms "and" and "or" shall be construed conjunctively or disjunctively, whichever makes the individual request more inclusive.

O.    The singular and masculine form of any noun or pronoun shall embrace and be read and applied as embracing the plural, the feminine, and the neuter, except where circumstances clearly make it inappropriate.

P.    "Infringed, " and any variant thereof, refers to any form of infringement actionable under United States law, including direct infringement, contributory infringement, inducement to infringe, literal infringement, and infringement under the doctrine of equivalents.

Q.     When requested to "Identify" or provide the "Identity" of a Person, please state with respect to each such Person:  (1) his, her, or its name; (2) his, her, or its present address; (3) his, her, or its telephone number; and (4) for an individual, his or her present or last known employer and his or her present or last known position with that employer.

R.     Whenever in these Interrogatories there is a request to "Identify" a Document or to provide the "Identity" of a Document, please set forth:  (1) the identity of the Person(s) who drafted the Document; (2) the Identity of the Person(s) who received (as addressee, "cc," "bcc," or otherwise) or approved the Document or a copy thereof; (3) the date of the Document; (4) the present location of the Document; (5) the present custodian of the Document; (6) the type of Document (e.g., letter, memorandum, tape recording, or other form of document); and (7) a description of the Document with the specificity required to allow it to be requested by a subpoena or a request for production of documents.

S.     "Concerning" means relating to, referring to, describing, discussing, depicting, evidencing, identifying or constituting.

T.     Each response shall include such information as is available to Symantec or within Symantec's custody, possession, or control, or the custody, possession, or control of Symantec's attorneys, investigators, agents, employees, or other representatives.  Documents within the possession, custody or control of Symantec means documents within the possession, custody or control of any current or former attorney, employee, partner, corporate parent, subsidiary, affiliate, agent, representative, officer, or director of Symantec, and other persons acting on Symantec's behalf.

U.     If, after exercising due diligence to secure the information requested, an individual Interrogatory or any part thereof cannot be fully answered, please state the reasons for the inability to fully answer, answer the individual Interrogatory to the fullest extent possible, and state what information, knowledge, or belief Symantec has concerning the unanswered portion.

3

V.    For any information deliberately withheld, please provide a written statement setting forth: (1) the identity of each Person from and to whom the information has been communicated; (2) a brief description of the subject matter of the information; and (3) the legal ground relied upon in withholding the information.

W.    If Symantec chooses to exercise the option to respond to any Interrogatory by producing business records pursuant to Rule 33(d), identify such business records by the interrogatory to which they are responsive.

X.    The terms "refer," "referring," "relate," or "relating" as used herein include, but are not limited to the following meanings: bearing upon, concerning, constituting, discussing, describing, evidencing, identifying, concerning, mentioning, in connection with, pertaining to, respecting, regarding, responding to, or in any way factually or logically relevant to the matter described in the request.

Y.    The term "Accused Products" shall mean all software products relating to computer network intrusion detection, prevention or analysis developed, made, used, sold or offered for sale in, or imported into the United States at any time from November 2001 to the present, including but not limited to ManHunt, Symantec Security Gateway, Symantec EventManager for Intrusion Protection, and Symantec Security Management System.

## INTERROGATORIES

INTERROGATORY NO. 1:

Identify by trade name and model name or number, including any internal identification numbers or parts numbers, each and every product that you have made, used, sold, licensed, offered for sale, imported into the United States, or have otherwise provided from November 2001 to the present that employs software or hardware directed to computer network intrusion detection, prevention or analysis, and for each such product, identify the range of dates during which you have sold, offered, licensed,

imported or otherwise provided or made available each of such version, model, and release of such product.

INTERROGATORY NO. 2:

Describe any consideration, plan or attempt by you, your suppliers, or others acting on your behalf to alter the Accused Products or the method, and/or process of using the Accused Products to avoid infringement or potential infringement of any of the patents-in-suit, such as by designing around the Patents-in-Suit, and identify the person(s) knowledgeable of and/or involved in such consideration, plan or attempt, and identify all documents which refer to or relate to such consideration, plan or attempt.

INTERROGATORY NO. 3:

Identify by name and address all persons, companies, or entities involved in the conception, design, development and testing of each Accused Product and describe in detail such activities.

INTERROGATORY NO. 4:

For each product identified in response to Interrogatory No. 1 that you contend does not infringe any of the claims of the Patents-in-Suit, specify each claim element or limitation that allegedly is not met by the product, the factual bases for that contention, and the three persons most knowledgeable about those facts. Your response may take the form of a claim chart.

INTERROGATORY NO. 5:

Provide your construction of each element of each claim of each of the patents-in-suit along with a chart specifically identifying and describing in detail any intrinsic or extrinsic evidence supporting such construction, including without limitation all relied upon citations to the claim language, the patent specification, and the prosecution history.

INTERROGATORY NO. 6:

If you contend that any claim of any of the Patents-in-Suit is invalid, identify the specific statutory bases for the invalidity (e.g., 35 U.S.C. § 102(a)), the factual bases for

5

that contention, any allegedly invalidating prior art or publications, where each element of the claim is found in the prior art or publications, and the three people most knowledgeable about the factual bases for your contention. Your response may take the form of a claim chart.

INTERROGATORY NO. 7:

State whether you have conducted, caused to be conducted, or received any information regarding any search, study, evaluation, investigation, opinion, advice, or assessment of the infringement, validity or enforceability of the Patents-in-Suit. If the answer is affirmative, with respect to each, identify the date it was requested, the identity of the person who requested it, the date on which it was received, the identity of the person who provided it, the identity of all persons who received it, the identity of all persons who performed the study, the form in which it was received (e.g., oral or written; draft or final), any documents that set forth its result, any prior art located or discussed in it, and whether you intend to rely upon it as a defense to SRI's claim of willful infringement.

INTERROGATORY NO. 8:

State the date on which you first learned of any of the Patents-in-Suit and for each Patent-in-Suit, identity of who at your company first learned of the patent, and the circumstances under which you first learned of the patent.

INTERROGATORY NO. 9:

For each product identified in response to Interrogatory No. 1, state separately by year the total number of units purchased or manufactured or sold by you, the actual or average manufacturing cost per unit or actual or average per unit sales price, your total gross profits from the product, your net profits before taxes for the product and your net profits after taxes from the product.

INTERROGATORY NO. 10:

6

Identify by name and address all persons, companies, or entities involved in the manufacture, assembly, marketing and distribution of each of the Accused Products, along with the total quantity of each such product that each entity manufactured, from 2001 to the present, and describe in detail such activities.

INTERROGATORY NO. 11:

State all facts supporting your contention that the Patents-in-Suit are unenforceable by reason of SRI's alleged inequitable conduct.

INTERROGATORY NO. 12:

Identify by name, address and telephone number, all customers or prospective customers to whom Symantec has presented, supplied, sampled, demonstrated, offered to sell, or sold any Accused Product or products containing same, from 2001 to the present.

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

INTERROGATORY NO. 13:

Identify and describe in detail all communications Symantec has had with any third party regarding any of the patents-in-suit, or this lawsuit.

Dated: June 23, 2005                    FISH & RICHARDSON P.C.


By: _____
                                    Timothy Devlin (#4241)
                                    John F. Horvath (#4557)
                                    FISH & RICHARDSON P.C.
                                    919 N. Market St., Ste. 1100
                                    P.O. Box 1114
                                    Wilmington, DE 19889-1114
                                    Telephone: (302) 652-5070
                                    Facsimile: (302) 652-0607

                                    Howard G. Pollack (CA Bar No. 162897)
                                    Michael J. Curley (CA Bar No. 230343)
                                    FISH & RICHARDSON P.C.
                                    500 Arguello Street, Suite 500
                                    Redwood City, California 94063
                                    Telephone: (650) 839-5070
                                    Facsimile: (650) 839-5071

                                    Attorneys for Plaintiff
                                    SRI INTERNATIONAL, INC.

Rogs to Symantec.doc

8

CERTIFICATE OF SERVICE

I hereby certify that on the 23rd day of June, 2005, a true and correct copy of the

**PLAINTIFF SRI INTERNATIONAL, INC.'S FIRST SET OF**

**INTERROGATORIES TO DEFENDANT SYMANTEC CORPORATION**

[NOS. 1–13] was caused to be served on the attorneys of record at the following

addresses as indicated:


**VIA HAND DELIVERY**
Richard K. Herrmann
Morris, James Hitchens & Williams Llp
222 Delaware Avenue, 10th Floor
Wilmington, DE  19801

Attorney for Defendant
SYMANTEC CORPORATION


**VIA HAND DELIVERY**
Richard L. Horwitz
David E. Moore
Potter Anderson & Corroon LLP
Hercules Plaza
1313 North Market Street, 6th Floor
P.O. Box 951
Wilmington, DE  19899

Attorneys for Defendant
INTERNET SECURITY SYSTEMS,
INC.


**VIA FEDERAL EXPRESS**
Paul S. Grewal
Day Casebeer Madrid & Batchelder, LLP
20300 Stevens Creek Boulevard, Suite 400
Cupertino, California  95014

Attorney for Defendant
SYMANTEC CORPORATION


**VIA FEDERAL EXPRESS**
Holmes Hawkins, III
King & Spalding
191 Peachtree Street, N.E.
Atlanta, GA  30303-1763

Attorneys for Defendant
INTERNET SECURITY SYSTEMS,
INC.


———————————————————
John F. Horvath


1

# EXHIBIT C

# REDACTED

# EXHIBIT
# D

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

| | |
|---|---|
| SRI INTERNATIONAL, INC., a California Corporation,<br><br>       Plaintiff and<br>       Counterclaim-Defendant,<br><br>      v.<br><br>INTERNET SECURITY SYSTEMS, INC., a Delaware corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia Corporation, and SYMANTEC CORPORATION, a Delaware corporation,<br><br>       Defendants and<br>       Counterclaim- Plaintiffs. | Civil Action No. 04-CV-1199 (SLR) |

## SYMANTEC CORPORATION'S SECOND SUPPLEMENTAL RESPONSES TO SRI INTERNATIONAL, INC.'S INTERROGATORIES NOS. 6 AND 11

Pursuant to Federal Rules of Civil Procedure 26 and 33, Defendant Symantec Corporation ("Symantec") supplements its responses to Plaintiff SRI International, Inc.'s ("SRI") Interrogatories Nos. 6 and 11.

### GENERAL RESPONSES

1.     Symantec's responses to SRI's First Set of Interrogatories are made to the best of Symantec's present knowledge, information and belief. Symantec's responses are subject to amendment and supplementation should future investigation indicate that amendment or supplementation is necessary. Symantec undertakes no obligation, however, to supplement or amend these responses other than as required by the Federal Rules of Civil Procedure and the Local Rules for the United States District Court for the District of Delaware.

2.     Symantec's responses to SRI's First Set of Interrogatories are made according to information currently in Symantec's possession, custody and control.

3.     To the extent that Symantec responds to SRI's First Set of Interrogatories by stating information that is private, business confidential, proprietary, trade secret or otherwise

240733

protected from disclosure pursuant to Federal Rule of Civil Procedure 26(c)(7) or Federal Rule of Evidence 501, Symantec will respond pursuant to the terms of the Protective Order in this case.

4.    Symantec reserves all objections or other questions as to the competency, relevance, materiality, privilege, or admissibility of any information, document or thing produced in response to SRI's Interrogatories as evidence in any subsequent proceeding or trial in this or any other action for any purpose whatsoever.

5.    Symantec reserves the right to object on any ground at any time to additional interrogatories that SRI may propound involving or relating to the same subject matter as SRI's First Set of Interrogatories.

## OBJECTIONS

Symantec incorporates the Objections contained in Symantec's Response to SRI's First Set of Interrogatories. The applicable foregoing general objections are incorporated into each of the specific objections and responses that follow. The stating of a specific objection or response shall not be construed as a waiver of Symantec's general objections.

SECOND SUPPLEMENTAL RESPONSES TO PLAINTIFF'S
INTERROGATORIES NOS. 6 AND 11

INTERROGATORY NO. 6:

If you contend that any claim of any of the Patents-in-Suit is invalid, identify the specific

statutory bases for the invalidity (e.g., 35 U.S .C. § 102(a)), the factual bases for that contention,

any allegedly invalidating prior art or publications, where each element of the claim is found in

the prior art or publications, and the three people most knowledgeable about the factual bases for

your contention. Your response may take the form of a claim chart.

SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 6:

Symantec objects to Interrogatory No. 6 to the extent that it requests the "three people

most knowledgeable about the factual bases for your contentions." This portion of the

interrogatory seeks the premature identification of the expert witnesses upon which Symantec

intends to rely. Symantec further objects that this Interrogatory is overbroad to the extent that it

requests information regarding claims that SRI has not asserted against Symantec in this

litigation. SRI provided Symantec with a list of claims-at-issue in the Sept. 27, 2005 letter from

Gina M. Steele to Jonathan D. Loeb. Symantec's responses are limited to the claims listed in

that letter.[1]  To the extent that SRI may later try to assert additional claims against Symantec,

such action by SRI would be highly prejudicial to Symantec. Symantec reserves the right to

supplement or modify these responses should SRI belatedly add claims.

---

[1] SRI's Sept. 27, 2005 letter stated: "Interrogatory No. 1. With regard to your request for the
claims SRI is asserting against Symantec, SRI states as follows: SRI asserts that Symantec has
infringed claims 1-23 of the '615 patent; claims 1-18, and 20-24 of the '212 patent; claims 1-5,
8-16, 18-22 of the '203 patent; and claims 1, 4, 11-18, 21 and 24 of the '338 patent." These
claims will be referred to herein as "the claims-at-issue."

3

Moreover, despite repeated requests, SRI has not provided specific contentions regarding the conception date(s) for the alleged "inventions" claimed in the patents-in-suit. Instead, SRI has provided an approximately one year date range for conception of the '338, '203, and '615 patents, and an approximately two year date range for conception of the '212 patent.[2] SRI's failure to substantively respond to Symantec's Interrogatory No. 4, which requested the date(s) of conception and reduction-to-practice for each alleged "invention" claimed in the patents-in-suit, has severely prejudiced Symantec. Consequently, the patentability of the claims-at-issue must be assessed in light of the state of the relevant art as of the filing date of the original application from which the patents issued. Symantec intends to present evidence at trial that establishes and broadly illustrates the state of the art in intrusion detection and network monitoring as of November 9, 1998. Symantec may rely upon publications, patents, percipient and expert testimony, and/or contemporaneous and predecessor products to reveal the state of such art at that time (or as of any earlier date if Plaintiff offers legally adequate proof of an earlier date of invention).

The information provided in Symantec's response is preliminary in nature and subject to modification and supplementation. For example, Symantec has only recently received limited documents from SRI relating to the development work that led to the patents-in-suit and certain prior art systems and references, which Symantec has begun to review. Symantec continues to develop and refine its understanding of the state of the art as additional relevant information is acquired during the course of ongoing discovery. Ongoing discovery efforts may identify

---

[2] *See* SRI International Inc.'s First Supplemental Response to Interrogatory Nos. 4-10 and 12 of Defendant Symantec Corporation's First Set of Interrogatories [Nos. 1-12], Supplemental Response to Interrogatory No. 4.

additional prior art references or embodiments that are relevant to the invalidity of the claims-in-suit. Symantec will supplement this response in a timely manner upon receipt of sufficient information relating to such additional prior art references or embodiments.

Symantec further objects that this interrogatory is premature because Symantec has not been provided with any understanding of SRI's proposed claim constructions, and therefore is unable to determine how SRI's proposed claim constructions inform the anticipation and obviousness contentions disclosed herein. Furthermore, the contentions set forth below are not based upon Symantec's proposed claim constructions. Symantec reserves the right to supplement and modify its invalidity contentions under 35 U.S.C. §§ 102 and 103 subject to the claim constructions advanced by SRI and Symantec pursuant to the Court's Scheduling Order, which specifies that "on January 20, 2006, the parties shall exchange lists of those claim terms that they believe need construction and their proposed claim construction of those terms" and that the "parties shall agree upon and file the Joint Claim Construction Statement on February 17, 2006, with the claim chart separately docketed." The complete scope of available prior art and its applicability to individual claims-at-issue will not be certain until the Court has construed the claims of the patents-in-suit. Symantec therefore further reserves the right to supplement and modify these contentions once the Court has construed the claims.

The accompanying prior art charts, attached hereto as Exhibits A-1 – A-23, reflect Symantec's current understanding of the primary prior art references and embodiments upon which it intends to rely to establish anticipation of the claims-in-suit under 35 U.S.C. § 102 and/or obviousness under 35 U.S.C. § 103. To the extent that a particular prior art reference or embodiment does not alone anticipate all the limitations of any one of the claims-in-suit as ultimately construed by the court, Symantec reserves the right to combine the references and/or

embodiments disclosed herein with other references and/or embodiments that may complement any such reference or embodiment, to the extent that one skilled in the art at the relevant point in time would have had motivation to create such a combination.

Moreover, due to the extremely large number of prior art references that invalidate the claims at issue, as well as SRI's failure to provide conception and reduction-to-practice dates, Symantec cannot possibly list every combination of art that renders the claims-at-issue invalid under 35 U.S.C. § 103, and reserves the right to present different combinations of references and/or embodiments, to the extent that one skilled in the art at the relevant point in time would have had motivation to create such a combination.

### Relevant Prior Art References Identified To Date

The knowledge of one skilled in the art as of Nov. 9, 1998 would have been informed by access to and appreciation of at least the following practices, publications, patents, and publicly available technologies, products, and systems. Symantec intends to rely upon these and similar references to establish the state of the anomaly detection, intrusion detection, network monitoring, and related arts prior to Nov. 9, 1998, and to establish that the claims-in-suit were anticipated under 35 U.S.C. § 102 or would have been obvious under 35 U.S.C. § 103 as of Nov. 9, 1998:

- All prior art of record in the file histories of the patents-in-suit; or identified in the Background of the Invention section of the patents-in-suit;

- All prior art references identified in Exhibits A-1 – A-23 attached hereto; and

- All prior art references produced to SRI at Bates ranges SYM_P_0067248 – SYM_P_0082525 and SYM_P_0498070 – SYM_P_0511901.

### Additional Technologies, Products and Systems

- Argus,

- Arpwatch,
- ASIM (Automated Security Incident Measurement),
- Berkeley Packet Filter,
- Borderguard,
- Bro,
- Cabletron's Spectrum,
- CIDF (Common Intrusion Detection Framework),
- Computer Associates Unicenter TNG,
- CSM (Cooperating Security Managers),
- DIDS (Distributed Intrusion Detection System),
- EMERALD,
- FireWall-1,
- GrIDS (Graph based Intrusion Detection System),
- Harris Corporation Stake Out,
- Haystack,
- HP OpenView, Network Node Manager, and NetMetrix,
- IDES,
- Internet standards,
- IP Filter,
- ISM (Internetwork Security Manager),
- Ji-Nao,
- Libpcap,
- MIDAS (Multics Intrusion Detection and Alerting System),
- NADIR (Network Anomaly Detection and Intrusion Reporter),
- NetRanger,
- NFR (Network Flight Recorder),
- NIDES,
- NIDX,
- NSM (Network Security Monitor),
- Raxco AUDIT,
- Stalker, NetStalker and WebStalker,
- Sun Network Management System (Solstice Site Manager, Solstice Domain Manager, Solstice Enterprise Manager, and Sun Net Manager),
- Tcpdump,
- TCP Wrapper,
- TIS Firewall Toolkit,
- Tivoli Enterprise Manager, and
- Wisdom & Sense.

7

## PRIOR ART REFERENCES THAT ANTICIPATE THE ASSERTED CLAIMS-

## AT-ISSUE

The prior art cited herein invalidates the claims at issue under 35 U.S.C. §102, as set forth

in detail in the representative charts attached as Exhibits A-1 – A-22 to this Supplemental

Response. The cover page of each chart provides citations to referenced prior art, as well as

citations to related prior art disclosures. Representative anticipatory references include:

- Exhibit A-1: "Emerald 1997" and the additional references listed on page 1 of Exhibit A-1;

- Exhibit A-2: "Emerald - CMAD" and the additional references listed on pages 1-2 of Exhibit A-2;

- Exhibit A-3: "Emerald - Conceptual Overview" and the additional references listed on pages 1-2 of Exhibit A-3;

- Exhibit A-4: "Emerald - Conceptual Design 1997" and the additional references listed on pages 1-2 of Exhibit A-4;

- Exhibit A-5: "Emerald - Live Traffic Analysis" and the additional references listed on page 1 of Exhibit A-5;

- Exhibit A-6: "Network NIDES" and the additional references listed on page 1 of Exhibit A-6;

- Exhibit A-7: "Ji-Nao" (includes "Ji-Nao" and "Ji-Nao slides") and the additional references listed on page 1 of Exhibit A-7;

- Exhibit A-8: "NSM" and the additional references listed on page 1 of Exhibit A-8;

- Exhibit A-9: "DIDS February 1991 and DIDS October 1991" and the additional references listed on pages 1-2 of Exhibit A-9;

- Exhibit A-10: "GrIDS 1996 and GrIDS 1997" and the additional references listed on page 1 of Exhibit A-10;

- Exhibit A-11: "NetRanger" (includes "NetRanger User Guide 1.3.1" and "NetRanger product") and the additional references listed on pages 1-2 of Exhibit A-11;

- Exhibit A-12: "RealSecure" and the additional references listed on page 1 of Exhibit A-12;

- Exhibit A-13: "Network Level Intrusion Detection;"

- Exhibit A-14: "U.S. Pat. No. 5,825,750" and the additional reference listed on page 1 of Exhibit A-14;

- Exhibit A-15: "Fault Detection in an Ethernet Network via anomaly detectors" and the additional references listed on page 1 of Exhibit A-15;

- Exhibit A-16: "Stake Out Network Surveillance" and the additional reference listed on page 1 of Exhibit A-16;

- Exhibit A-17: "HP OpenView" and the additional references listed on pages 1-2 of Exhibit A-17;

- Exhibit A-18: "ISM" and the additional reference listed on page 1 of Exhibit A-18;

- Exhibit A-19: "Emerald 1997, Intrusive Activity 1991, NIDES 1994;"

- Exhibit A-20: Netstalker and HP OpenView" and the additional references listed on page 2 of Exhibit A-20;

- Exhibit A-21: "Network Flight Recorder" and the additional references listed on pages 1-2 of Exhibit A-21; AND

- Exhibit A-22: "AIS."

Citations to particular pages of a prior art reference in the attached prior art charts are to be understood as exemplary. Other pages of a prior art reference may also be relevant to the existence of a claim element, and Symantec reserves its right to supplement the page citations provided, if necessary. Symantec further reserves the right to supplement its § 102 contentions with additional prior art references because Symantec's investigation is still preliminary.

## PRIOR ART REFERENCES THAT RENDER THE CLAIMS-AT-ISSUE
## OBVIOUS

In addition to anticipating the claims- at-issue, a very large number of combinations of the prior art references identified render some or all of the claims-at-issue obvious under 35 U.S.C. § 103. Representative examples of invalidating combinations of the prior art references are identified below. Symantec reserves the right to establish that any alleged "invention" claimed in the patents-in-suit would have been obvious and thus invalid under 35 U.S.C. § 103 based upon any combination of references identified herein, or similar to those identified herein, that one skilled in the art as of Nov. 9, 1998 would have had motivation to create.

9

- Exhibit A-2: "Emerald - CMAD" (for indicated claims);

- Exhibit A-3: "Emerald - Conceptual Overview" (for indicated claims);

- Exhibit A-4: "Emerald - Conceptual Design 1997" (for indicated claims);

- Exhibit A-17: "HP OpenView" (see page 2 of Exhibit A-17 regarding § 103 combinations);

- Exhibit A-18: "ISM" (see page 1 of Exhibit A-18 regarding § 103 combinations);

- Exhibit A-19: "Emerald 1997, Intrusive Activity 1991, NIDES 1994" (see page 1 of Exhibit A-19 regarding § 103 combinations);

- Exhibit A-20: "NetStalker and HP OpenView" (see page 2 of Exhibit A-20 regarding § 103 combinations);

- Exhibit A-21: "Network Flight Recorder" (for indicated claims);

- Exhibit A-23: Summary chart of other relevant prior art, listing, for each individual limitation of each claim-at-issue, the prior art references that satisfy each limitation and could be combined with any of the references listed in Exhibits A-1 – A-22.

Symantec has provided as Exhibit A-23 a chart indicating prior art references disclosing particular limitations of each claim-at-issue. Given the large number of combinations, Symantec cannot identify all of the possible permutations at this time. For each of the prior art charts listed above for anticipation and/or obviousness, any missing claims or limitations could be satisfied by combining the cited reference of the prior art chart with reference(s) from Exhibit A-23. Symantec reserves the right to combine the cited references in any combination or permutation that one of skill in the art as of Nov. 9, 1998 would have had motivation to create or evaluate. Symantec further reserves the right to supplement its § 103 contentions with additional prior art references because Symantec's investigation is still preliminary.

## THE CLAIMS-AT-ISSUE ARE INVALID PURSUANT TO 35 U.S.C. § 112

The claims-at-issue are also invalid for failure to satisfy the best mode requirement under 35 U.S.C. § 112. SRI submitted source code in an Appendix to the patents-in-suit. A

10

preliminary examination of the source code provided in the Appendix indicates that the code in the Appendix is not the complete program that existed at the time. For example, the Appendix code would not compile and run. In addition, the Appendix code contains no configuration files allowing for the use of any particular network traffic data categories. Furthermore, the Appendix code does not appear to have code for a resolver or an expert system. On information and belief, Symantec believes discovery will show that SRI had a more complete set of source code by the time it filed U.S. Patent Application No. 09/188,739 and withheld much of that code from the Patent Office. That withheld code reflected the inventors' best mode of practicing the claims-at-issue.

In addition, the patents-in-suit are invalid for failure to satisfy the enablement and written description requirements of 35 U.S.C. § 112. Furthermore, the claims-at-issue are invalid as indefinite because the claims fail to particularly point out and distinctly claim the subject matter of the invention.

Symantec's contentions regarding the invalidity of SRI's patents-in-suit pursuant to 35 U.S.C. § 112 are preliminary and subject to modification and review. For example, Symantec has not yet had the opportunity to depose either of the inventors. Furthermore, document production is still ongoing and Symantec has only begun its review of SRI's documents. In addition, despite Symantec's July 15, 2005 request for the production of SRI source code relevant to the patents-at-issue, SRI has not yet made any such source code available to Symantec.[3]

---

[3] See Symantec Corporation's First Set of Requests for Production of Documents to SRI International, Inc., RFP No. 31 (July 15, 2005).

INTERROGATORY NO. 11:

State all facts supporting your contention that the Patents-in-Suit are unenforceable by reason of SRI's alleged inequitable conduct.

SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 11:

Symantec objects to this Interrogatory on the grounds that it is unduly burdensome because Symantec has already identified facts supporting its contentions regarding inequitable conduct in Symantec's Answer and Counterclaims to SRI International, Inc.'s First Amended Complaint filed on May 23, 2005. In addition, discovery has just begun in the case. Ongoing discovery efforts may identify additional facts showing the unenforceability of the patents-in-suit. Symantec will supplement this response in a timely manner upon receipt of additional relevant information. Subject to and without waiving the foregoing general and specific objections, Symantec responds by incorporating by reference paragraphs 40-41 of Symantec's Answer of May 23.

Symantec further responds with the following facts:

To the extent now known, and subject to further clarification as to the full extent of the withholding and misrepresentation of information, the inventors and/or their agents made a number of misrepresentations or omissions of material fact to the U.S. Patent Office, including but not limited to omissions regarding prior art.

"Network NIDES"

Intentional and material false statements or omissions were made by the inventors and/or their agents by the failure by applicants to disclose to the Examiner one of the inventor's own material prior art publications: *Next-generation Intrusion Detection Expert Systems (NIDES): A Summary*, by Debra Anderson, Thane Frivold, and Alfonso Valdes, SRI-CSL-95-07, May 1995

(hereinafter "*Network NIDES*"). In addition to the facts alleged in paragraphs 40-41 of

Symantec's answer, the materiality of this reference is demonstrated by the "Network NIDES"

chart at Exhibit A-6, which indicates that the reference anticipates most of the claims-at-issue. It

is also demonstrated by SRI's submission of the Network NIDES reference to the PTO during

the prosecution of pending patent applications, U.S. Patent Application Nos. 10/429,611 and

10/805,729, which are related to the patents-in-suit.

In addition, intentional and material false statements or omissions were made by the

inventors and/or their agents by the failure by applicants to disclose to the Examiner several

additional prior art publications with disclosures similar to the disclosure of *Network NIDES*:

- T. Lunt, A. Tamaru, F. Gilham, R. Jagannathan, P.G. Neumann, and C. Jalali, *IDES: A*

  *Progress Report*, in Proceedings of the 6th Annual Computer Security Applications

  Conference, 1990 [SYM_P_0080629- SYM_P_0080641]. Relevant information from this

  publication includes, but is not limited to, the following:

  > "8.5 Monitoring Network Traffic
  > The theoretical basis for IDES can be extended so as to enable the
  > development of an IDES that could monitor traffic in tactical
  > communication networks to detect suspicious activity. The required
  > extensions are twofold. ... Second, IDES's rule base has been designed for
  > detecting suspicious *user* activity. To use IDES to monitor network
  > traffic, where user data are not available, we must create a rule base with a
  > set of rules specific to the domain of detecting suspicious network traffic
  > patterns.
  > In addition to establishing the theoretical foundation for these two
  > extensions to IDES, we would develop candidate architectures for
  > incorporating one or more IDES into the network topology. So far IDES
  > has assumed centralized control and is thus appropriate for systems with
  > high channel capacity and low transfer delay. Tactical networks operating
  > under stress are expected to have neither. Moreover, tactical networks can
  > become partitioned, so that an IDES with centralized control would not
  > have global knowledge. Thus, a distributed approach to detect anomalous
  > behavior is more appropriate for tactical communications networks. We

envision that IDES in this context would consist of a set of loosely
coupled IDES machines." *Id.* at 283 [SYM_P_0080639].

• T.F. Lunt, A. Tamaru, F. Gilham, R. Jagannathan, C. Jalali, H.S. Javitz, A. Valdes, and P.G.

Neumann, *A Real-Time Intrusion-Detection Expert System (IDES)*, Interim Progress Report,

Project 6784, SRI International, May 1990 [SYM_P_0078995- SYM_P_0079133].

Relevant information from the publication includes, but is not limited to, the following:

"9.2.4 Monitoring Network Traffic
The theoretical basis for IDES can be extended so as to enable the
development of an IDES that could monitor traffic in tactical
communication networks to detect suspicious activity. The required
extensions are threefold.
1. IDES's statistical algorithms are based on the probabilities of
occurrence of the events it observes. In a network, however, IDES would
not be able to operate with global knowledge. Thus, IDES's algorithms
must be extended to give meaningful results when some information is
missing and probabilities can only be estimated.
2. IDES's rule base has been designed for detecting suspicious *user*
activity. To use IDES to monitor network traffic, where user data are not
available, we must create a rule base with a set of rules specific to the
domain of detecting suspicious network traffic patterns.
3. IDES's statistical and rule-based components can be enhanced using
ideas from visual pattern recognition theory, machine learning, neural
networks (considered below), and other artificial intelligence techniques.
This will enhance IDES's ability to make inferences about the type and
location of suspicious activity by observing traffic.
In addition to establishing the theoretical foundations for these three
extensions to IDES, we would develop candidate architectures for
incorporating one, or more, IDES into the network topology. So far IDES
has assumed centralized control and is thus appropriate for systems with
high channel capacity and low transfer delay. Tactical networks operating
under stress are expected to have neither. Moreover, tactical networks can
become partitioned, so that an IDES with centralized control would not
have global knowledge. Thus, a distributed approach to detect anomalous
behavior is more appropriate for tactical communications networks. We
envision that IDES in this context would consist of a set of loosely
coupled IDES machines." *Id.* at 82-83 [SYM_P_0079085 –
SYM_P_0079086].

14

* T. F. Lunt, A. Tamaru, F. Gilham, R. Jagannathan, P. G. Neumann, H. S. Javitz, A. Valdes,

and T. D. Garvey, *A Real-Time Intrusion Detection Expert System (IDES) -- Final Technical*

*Report*, Tech. Rep., SRI Computer Science Laboratory, SRI International, Menlo Park, CA,

Feb. 1992 [SYM_P_0079206- SYM_P_0079370]. Relevant information from the

publication includes, but is not limited to, the following:

> "Detecting Network Intrusions  Current computing environments are,
> more and more, massively networked sets of workstations, servers,
> mainframes, supercomputers, and special-purpose machines and devices.
> Focusing on the vulnerabilities of any single host or even any single
> homogenous local network of machines may prove inadequate in such a
> distributed environment.  Detecting intruders will require a comprehensive
> view of a network, possibly extending to other networks connected to the
> local network.  Applying IDES technology to this (possibly
> heterogeneous) computing environment will require expanding the scope
> of IDES to include the ability to detect network intrusions as well as
> intrusions into the individual host machines.  To achieve this, the
> following steps are necessary:
> * Build a rule base into IDES that contains specialized knowledge
>   about network vulnerabilities and intrusion scenarios.
> * Enable IDES to work with partial information, since in a very large
>   network it is unlikely that IDES will possess complete information
>   about the whole network at all times.  This capability will make
>   IDES especially attractive for use in tactical communication
>   networks, which must operate in hostile environments.
> * Develop an overall architecture for inserting IDES or a distributed
>   set of component IDES machines into a large, complex network....
> * Network Intrusion Detection – We plan to develop and implement
>   a capability for detecting network intrusions by combining a
>   specialized rule base on network vulnerabilities with intrusion
>   scenarios, develop a capability for the detection of intrusions with
>   partial information, and develop an architecture for the integration
>   of IDES into a large, complex network.
> * Large Network Architecture – We plan to develop an architecture
>   for inserting IDES into a large network, and will we [sic] work
>   with a U.S. Government installation (e.g., NOSC) to install IDES
>   in such an environment." *Id.* at 95-97 [SYM_P_0079308 – SYM
>   _P_0079310].

> "9.3 Monitoring Network Traffic

We also plan to extend the theoretical basis for IDES to enable the
development of an IDES that could monitor traffic in tactical
communication networks to detect suspicious activity. The required
extensions are twofold: ...

- IDES's rule base has been designed for detecting suspicious *user*
  activity. To use IDES to monitor network traffic, where user data
  are not available, we must create a rule base with a set of rules
  specific to the domain of detecting suspicious network traffic
  patterns.

In addition to establishing the theoretical foundation for these extensions
to IDES, we plan to develop candidate architectures for incorporating one
or more IDES into the network topology. So far IDES has assumed
centralized control and is thus appropriate for systems with high channel
capacity and low transfer delay. Tactical networks operating under stress
are expected to have neither. Moreover, tactical networks can become
partitioned, so that an IDES with centralized control would not have
global knowledge. Thus, a distributed approach to detect anomalous
behavior is more appropriate for tactical communications networks. We
envision that IDES in this context would consist of a set of loosely
coupled IDES machines." *Id.* at 103-04 [SYM_P_0079316 –
SYM_P_0079317].


In addition to failing to submit these references, SRI also failed to disclose to the Patent

Office several § 102(b) references concerning the EMERALD project, the very project under

which SRI performed the work that led to the filing of the patents-in-suit, as indicated by the

referenced DARPA contract number in the specification of the patents-in-suit. These references

include a paper for and presentation at the November 1996 CMAD Workshop ("Emerald –

CMAD"), a Conceptual Overview paper, which was posted on SRI's website more than a year

before the priority date of the patents-in-suit ("Emerald – Conceptual Overview"), and the

Emerald Conceptual Design and Planning Document ("Emerald – Conceptual Design 1997"),

which also was posted on SRI's website more than a year before the priority date of the patents-

in-suit. The citations to these documents are found in the cover pages to Exhibits A-1 – A-4.

The materiality of these references is demonstrated by the prior art invalidity charts attached as

Exhibits A2 - A4. Moreover, much of the specification of the patents-in-suit can be traced to the

16

disclosures in these references. All of these references were co-authored by one or more of the named inventors. Yet, none of them were cited to the Examiner.

The omitted *Network NIDES* reference, the three IDES references cited above, and the additional Emerald references cited above, would have been considered by a reasonable examiner to be material to a determination of patentability of the claims of the patents-in-suit, and on information and belief, said omissions were made with intent to deceive the U.S. Patent Office. Had the inventors and/or their agents made accurate representations to the U.S. Patent Office, the patents-in-suit would not have issued. Thus, the patents-in-suit are unenforceable for inequitable conduct.

## "NSM"

In addition, intentional and material false statements or omissions were made by the inventors and/or their agents by the failure by applicants to disclose to the Examiner during prosecution of the '338 patent any publications regarding the Network Security Monitor ("NSM") including: L.T. Heberlein, G.V. Dias, K. N. Levitt, B. Mukherjee, J. Wood, D. Wolber., *A Network Security Monitor*, Proc. 1990 Symposium on Research in Security and Privacy, pp. 296-304, May 1990 [SYM_P_0068974 - SYM_P_0068956] and further including the additional references listed on page 1 of Exhibit A-8. The materiality of this reference is demonstrated by the "NSM" chart at Exhibit A-8, which indicates that the reference anticipates most of the claims-at-issue for the '338 patent.

The inventors were aware of the existence of the NSM system at least as early as May 1997. Phillip Porras was the co-author on a publication discussing NSM dated May 16, 1997,

*see* [SRI012308-012404 at 012390].[4]  In addition, P. Porras and P. Neumann, *EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances*, 20th NISSC October 9, 1997 [SYM_P_0068831- SYM_P_0068843] states that "the Network Security Monitor [7] seeks to analyze packet data rather than conventional audit trails..." *id.* at [SYM_P_0068842].

The omitted *Network Security Monitor* May 1990 reference, as well as the related references listed on page one of Exhibit A-8, would have been considered by a reasonable examiner to be material to a determination of patentability of the '338 patent claims, and on information and belief, said omissions were made with intent to deceive the U.S. Patent Office. Had the inventors and/or their agents made accurate representations to the U.S. Patent Office, the '338 patent would not have issued.  Thus, the '338 patent is unenforceable for inequitable conduct.

"Ji-Nao"

Intentional and material false statements or omissions were made by the inventors and/or their agents by the failure by applicants to disclose to the Examiner during prosecution of the patents-in-suit any publications regarding the Ji-Nao system, including:

- Y. Frank Jou et al., *Architecture Design of a Scalable Intrusion Detection System for the Emerging Network*, Technical Report CDRL A005, DARPA Order No. E296, Dept. of Computer Science North Carolina State University, April 1997 [SYM_P_0070541 – SYM_P_0070582].

---

[4] SRI has marked this document as "CONFIDENTIAL – Subject to Protective Order."  However, the document itself indicates that it was publicly posted on the Internet at http://www.csl.sri.com/intrusion.html.  Symantec believes this document has been improperly designated as Confidential.  However, in an abundance of caution, Symantec has marked as Confidential Exhibit A-4, which provides the anticipatory disclosures of this document.

- Y. Frank Jou and S. Felix Wu, *Scalable Intrusion Detection for the Emerging Network Infrastructure*, IDS Program Review, SRI, July 1997 [SYM_P_0503679 – SYM_P_0503709].

These references, as well as the related references listed on page 1 of Exhibit A-7, would have been considered by a reasonable examiner to be material to a determination of patentability of the claims of the patents-in-suit. The materiality of these references is demonstrated by the "Ji-Nao" and "Ji-Nao slides" charts at Exhibit A-7, which indicates that both references anticipate the claims-at-issue of the patents-in-suit. The Ji-Nao system actually used the NIDES algorithms from SRI to perform statistical analysis: "the NIDES project at SRI is most extensive in its scope and development. It also has the most complete documentations available to the general public. With the understanding of statistical analysis's general applicability, we will adapt NIDES's statistical algorithm in our approach as a starting point and modify it as necessary." *See* Y. Frank Jou et al., *Architecture Design of a Scalable Intrusion Detection System for the Emerging Network*, Technical Report CDRL A005, DARPA Order No. E296, Dept. of Computer Science North Carolina State University, April 1997 at p. 18 [SYM_P_0070563].

The inventors were aware of the existence of the Ji-Nao system at least as early as November 1996. On information and belief, on November 12-14, 1996 at the CMAD IV Computer Misuse and Anomaly Detection Conference in Monterey, California, the inventors of the patents-in-suit presented the subject matter of the patents-in-suit during the same session as a presentation on the Ji-Nao system. During Session 4, Phillip Porras and Alfonso Valdes presented *Analysis and Response for Intrusion Detection in Large Networks*, a reference clearly related to the subject matter of the patents-in-suit because the conference summary discusses the

19

Emerald system on which the patents-in-suit are based and is an anticipatory reference, see Exhibit A-2. During this same session, Y. Frank Jou of MCNC presented *Scalable Intrusion Detection for the Emerging Network Infrastructure* [SYM_P_0500920 – SYM_P_0500969 at SYM_P_0500968]. *Scalable Intrusion Detection for the Emerging Network Infrastructure* was the title of multiple anticipatory references describing the Ji-Nao system, see Exhibit A-7.

Moreover, on information and belief, the named inventors were collaborating with Mr. Jou and his team. Mr. Porras prepared a December 16, 1996 quarterly report to Rome Laboratory, the governmental agency that was responsible for monitoring SRI's work under the DARPA contract for the EMERALD project, which references working with Mr. Jou of the Ji-Nao team. [SRI 11739-43].[5] In addition, Mr. Porras indicated in the May 20, 1997 *Conceptual Design and Planning for Emerald* document (see Exhibit A-4) that the Ji-Nao team at MCNC was using SRI's statistical profiler engine. [SRI 012308-12404 at SRI 012400[6]].

Furthermore, on information and belief, the Ji-Nao slides shown to be anticipatory in Exhibit A-7 were presented at SRI in July of 1997. *See* the Internet Archive of the MCNC website, listing the Ji-Nao slides as "Project Update Viewgraph (at SRI, July 97, powerpoint)" [SYM_P_0071957], see also [SYM_P_0499511 – SYM_P_0499601 at SYM_P_0499570].

In addition, on February 25-27, 1997, at the Intrusion Detection PI meeting in Savannah, Georgia Phillip Porras presented on SRI's Emerald system during the same day as Frank Jou of MCNC presented on the Ji-Nao system. *See* Feb. 21, 1997 email from Joe Daniero "re: tentative agenda for Intrusion Detection Meeting – Savannah" [SYM_P_0076782 – SYM_P_0076786 at

---

[5] SRI has marked this document "Confidential – Subject to Protective Order."

[6] Symantec believes SRI has improperly marked this document as Confidential. *See supra* note 4.

20

0076783].

In addition, correspondence from Phillip Porras regarding the Common Intrusion

Detection Framework (CIDF) indicates that the Emerald team from SRI and the Ji-Nao team

from MCNC and North Carolina State University worked closely together on the CIDF effort.

*See* July 22, 1997 email from Phillip A. Porras to cidf@cs.ucdavis.edu entitled "A Common

Intrusion-Detection Interface Specification Version 2.0 by Emerald/JiNao Groups (SRI,

MCNC/NCSU)" [SYM_P_0500624 – SYM_P_0500639].  See also "The DARPA Common

Intrusion Detection Framework – The CIDF Working Group" [SYM_P_0071467 –

SYM_P_0071470].

The omitted Ji-Nao references would have been considered by a reasonable examiner to

be material to a determination of patentability of the claims of the patents-in-suit, and on

information and belief, said omissions were made with intent to deceive the U.S. Patent Office.

Had the inventors and/or their agents made accurate representations to the U.S. Patent Office, the

patents-in-suit would not have issued.  Thus, the patents-in-suit are unenforceable for inequitable

conduct.

Dated:  November 15, 2005                          DAY CASEBEER
                                                  MADRID & BATCHELDER LLP


                                            By:  _Paul S. Grewal_____
                                                        Paul S. Grewal


                                            Paul S. Grewal (*pro hac vice*)
                                            Day Casebeer Madrid & Batchelder LLP
                                            20300 Stevens Creek Blvd., Suite 400


21

Cupertino, CA 95014
Tel: (408) 873-0110
Fax: (408) 873-0220

*Attorneys for Defendant and Counterclaim-
Plaintiff* Symantec Corporation

OF COUNSEL:

Lloyd R. Day, Jr. (*pro hac vice*)
Robert M. Galvin (*pro hac vice*)
Paul S. Grewal (*pro hac vice*)
Day Casebeer Madrid & Batchelder LLP
20300 Stevens Creek Blvd., Suite 400
Cupertino, CA 95014
Tel: (408) 873-0110
Fax: (408) 873-0220

Michael J. Schallop (*pro hac vice*)
Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
Tel: (408) 517-8000
Fax: (408) 517-8121

Dated: November 15, 2005

22

# EXHIBIT
# E

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

| | |
|---|---|
| SRI INTERNATIONAL, INC., a California Corporation,<br><br>       Plaintiff and<br>       Counterclaim-Defendant,<br><br>  v.<br><br>INTERNET SECURITY SYSTEMS, INC., a Delaware corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia Corporation, and SYMANTEC CORPORATION, a Delaware corporation,<br><br>       Defendants and<br>       Counterclaim- Plaintiffs. | Civil Action No. 04-CV-1199 (SLR) |

## SYMANTEC CORPORATION'S FOURTH SUPPLEMENTAL RESPONSE TO SRI INTERNATIONAL, INC.'S INTERROGATORY NO. 6

Pursuant to Federal Rules of Civil Procedure 26 and 33, Defendant Symantec Corporation ("Symantec") supplements its responses to Plaintiff SRI International, Inc.'s ("SRI") Interrogatory No. 6.

### GENERAL RESPONSES

1.     Symantec's responses to SRI's First Set of Interrogatories are made to the best of Symantec's present knowledge, information and belief. Symantec's responses are subject to amendment and supplementation should future investigation indicate that amendment or supplementation is necessary. Symantec undertakes no obligation, however, to supplement or amend these responses other than as required by the Federal Rules of Civil Procedure and the Local Rules for the United States District Court for the District of Delaware.

2.     Symantec's responses to SRI's First Set of Interrogatories are made according to

273698_1

1

information currently in Symantec's possession, custody and control.

3.    To the extent that Symantec responds to SRI's First Set of Interrogatories by

stating information that is private, business confidential, proprietary, trade secret or otherwise

protected from disclosure pursuant to Federal Rule of Civil Procedure 26(c)(7) or Federal Rule

of Evidence 501, Symantec will respond pursuant to the terms of the Protective Order in this

case.

4.    Symantec reserves all objections or other questions as to the competency,

relevance, materiality, privilege, or admissibility of any information, document or thing

produced in response to SRI's Interrogatories as evidence in any subsequent proceeding or trial

in this or any other action for any purpose whatsoever.

5.    Symantec reserves the right to object on any ground at any time to additional

interrogatories that SRI may propound involving or relating to the same subject matter as SRI's

First Set of Interrogatories.

## OBJECTIONS

Symantec incorporates the Objections contained in Symantec's Response to SRI's First

Set of Interrogatories. The applicable foregoing general objections are incorporated into each of

the specific objections and responses that follow. The stating of a specific objection or response

shall not be construed as a waiver of Symantec's general objections.

### THIRD SUPPLEMENTAL RESPONSE TO PLAINTIFF'S
### INTERROGATORY NO. 6

**INTERROGATORY NO. 6:**

If you contend that any claim of any of the Patents-in-Suit is invalid, identify the specific

statutory bases for the invalidity (e.g., 35 U.S.C. § 102(a)), the factual bases for that contention,

any allegedly invalidating prior art or publications, where each element of the claim is found in

2

the prior art or publications, and the three people most knowledgeable about the factual bases for

your contention. Your response may take the form of a claim chart.

## SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 6:

Symantec objects to Interrogatory No. 6 to the extent that it requests the "three people

most knowledgeable about the factual bases for your contentions." This portion of the

interrogatory seeks the premature identification of the expert witnesses upon which Symantec

intends to rely. Symantec further objects that this Interrogatory is overbroad to the extent that it

requests information regarding claims that SRI has not asserted against Symantec in this

litigation. SRI provided Symantec with a list of claims-at-issue in the Sept. 27, 2005 letter from

Gina M. Steele to Jonathan D. Loeb.[1] However, SRI later asserted additional claims in its

"Second Supplemental Responses to Defendant Symantec's First Set of Interrogatories [Nos. 1-

12]," received by Symantec on November 21, 2005.[2] The addition of these claims at such a late

date is prejudicial to Symantec. To the extent that SRI may later try to assert still more

additional claims against Symantec, such action by SRI would again be highly prejudicial to

Symantec. Symantec reserves the right to supplement or modify these responses should SRI

belatedly add additional claims.

Symantec has not yet had an opportunity to explore through discovery the factual

---

[1] SRI's Sept. 27, 2005 letter stated: "Interrogatory No. 1. With regard to your request for the claims SRI is asserting against Symantec, SRI states as follows: SRI asserts that Symantec has infringed claims 1-23 of the '615 patent; claims 1-18, and 20-24 of the '212 patent; claims 1-5, 8-16, 18-22 of the '203 patent; and claims 1, 4, 11-18, 21 and 24 of the '338 patent."

[2] Specifically, claims 2, 3, 5-8, 10, 19, and 25 of the '338 patent, claims 6, 7, and 17 of the '203 patent, claim 19 of the '212 patent, and claims 34-43, 44-53, 64-73, and 84-93 were all belatedly asserted against Symantec in SRI's "Second Supplemental Responses to Defendant Symantec's First Set of Interrogatories [Nos. 1-12]." These claims, together with the claims identified in SRI's Sept. 27, 2005 letter, will be referred to herein as "the claims-at-issue."

predicates underlying SRI's claimed conception dates for the alleged inventions. Consequently, the patentability of the claims-at-issue must be assessed in light of the state of the relevant art as of the filing date of the original application from which the patents issued. Symantec intends to present evidence at trial that establishes and broadly illustrates the state of the art in intrusion detection and network monitoring on or before November 9, 1998. Symantec may rely upon publications, patents, percipient and expert testimony, and/or contemporaneous and predecessor products to reveal the state of such art at that time (or as of any earlier date if Plaintiff offers legally adequate proof of an earlier date of invention).

The information provided in Symantec's response is preliminary in nature and subject to modification and supplementation. For example, Symantec has only recently received limited documents from SRI relating to the development work that led to the patents-in-suit and certain prior art systems and references, which Symantec has begun to review. Symantec has not yet had an opportunity to depose the individuals involved in the conception and reduction-to-practice of the alleged inventions. Symantec continues to develop and refine its understanding of the state of the art as additional relevant information is acquired during the course of ongoing discovery. Ongoing discovery efforts may identify additional prior art references or embodiments that are relevant to the invalidity of the claims-in-suit. Symantec will supplement this response in a timely manner upon receipt of sufficient information relating to such additional prior art references or embodiments.

Symantec further objects that this interrogatory is premature because Symantec has not been provided with any understanding of SRI's proposed claim constructions, and therefore is unable to determine how SRI's proposed claim constructions inform the anticipation and

4

obviousness contentions disclosed herein. Furthermore, the contentions set forth below are not based upon Symantec's proposed claim constructions. Symantec reserves the right to supplement and modify its invalidity contentions under 35 U.S.C. §§ 102 and 103 subject to the claim constructions advanced by SRI and Symantec pursuant to the Court's Scheduling Order, which specifies that "on January 20, 2006, the parties shall exchange lists of those claim terms that they believe need construction and their proposed claim construction of those terms" and that the "parties shall agree upon and file the Joint Claim Construction Statement on February 17, 2006, with the claim chart separately docketed." The complete scope of available prior art and its applicability to individual claims-at-issue will not be certain until the Court has construed the claims of the patents-in-suit. Symantec therefore further reserves the right to supplement and modify these contentions once the Court has construed the claims.

The accompanying prior art charts, attached hereto as Exhibits A-1 – A-23, reflect Symantec's current understanding of the primary prior art references and embodiments upon which it intends to rely to establish anticipation of the claims-in-suit under 35 U.S.C. § 102 and/or obviousness under 35 U.S.C. § 103. To the extent that a particular prior art reference or embodiment does not alone anticipate all the limitations of any one of the claims-in-suit as ultimately construed by the court, Symantec reserves the right to combine the references and/or embodiments disclosed herein with other references and/or embodiments that may complement any such reference or embodiment, to the extent that one skilled in the art at the relevant point in time would have had motivation to create such a combination.

Moreover, due to the extremely large number of prior art references that invalidate the claims at issue, Symantec cannot possibly list every combination of art that renders the claims-at-issue invalid under 35 U.S.C. § 103, and reserves the right to present different combinations of

5

references and/or embodiments, to the extent that one skilled in the art at the relevant point in time would have had motivation to create such a combination.

### Relevant Prior Art References Identified To Date

The knowledge of one skilled in the art as of Nov. 9, 1998 would have been informed by access to and appreciation of at least the following practices, publications, patents, and publicly available technologies, products, and systems. Symantec intends to rely upon these and similar references to establish the state of the anomaly detection, intrusion detection, network monitoring, and related arts on or before Nov. 9, 1998, and to establish that the claims-in-suit were anticipated under 35 U.S.C. § 102 or would have been obvious under 35 U.S.C. § 103 on or before Nov. 9, 1998:

- All prior art of record in the file histories of the patents-in-suit; or identified in the Background of the Invention section of the patents-in-suit;

- All prior art references identified in Exhibits A-1 – A-23 attached hereto; and

- All prior art references produced to SRI at Bates ranges SYM_P_0067248 – SYM_P_0082535; SYM_P_0499257 – SYM_P_0506549; SYM_P_0511902-SYM_P_0513006; SYM_P_0526260 – SYM_P_0531122; SYM_P_0531123 – SYM_P_0531139; SYM_P_0534104 – SYM_P_0534116; SYM_P_0535194 – SYM_P_0535341.

### Additional Technologies, Products and Systems

- Argus,
- Arpwatch,
- ASIM (Automated Security Incident Measurement),
- Berkeley Packet Filter,
- Borderguard,
- Bro,
- Cabletron's Spectrum,
- CIDF (Common Intrusion Detection Framework),
- Computer Associates Unicenter TNG,
- CSM (Cooperating Security Managers),
- DIDS (Distributed Intrusion Detection System),

- EMERALD,
- FireWall-1,
- GrIDS (Graph based Intrusion Detection System),
- Harris Corporation Stake Out,
- Haystack,
- HP OpenView, Network Node Manager, and NetMetrix,
- IDES,
- Internet standards,
- IP Filter,
- ISM (Internetwork Security Manager),
- Ji-Nao,
- Libpcap,
- MIDAS (Multics Intrusion Detection and Alerting System),
- NADIR (Network Anomaly Detection and Intrusion Reporter),
- NetRanger,
- NFR (Network Flight Recorder),
- NIDES,
- NIDX,
- NSM (Network Security Monitor),
- Raxco AUDIT,
- Stalker, NetStalker and WebStalker,
- Sun Network Management System (Solstice Site Manager, Solstice Domain Manager, Solstice Enterprise Manager, and Sun Net Manager),
- SunScreen,
- Tcpdump,
- TCP Wrapper,
- TIS Firewall Toolkit,
- Tivoli Enterprise Manager, and
- Wisdom & Sense.

## PRIOR ART REFERENCES THAT ANTICIPATE THE ASSERTED CLAIMS-AT-ISSUE

The prior art cited herein invalidates the claims at issue under 35 U.S.C. §102, as set forth in detail in the representative charts attached as Exhibits A-1 – A-22 to this Supplemental Response. The cover page of each chart provides citations to referenced prior art, as well as citations to related prior art disclosures. Representative anticipatory references include:

- Exhibit A-1: "Emerald 1997" and the additional references listed on page 1 of Exhibit A-1;

- Exhibit A-2: "Emerald - CMAD" and the additional references listed on pages 1-2 of Exhibit A-2;

- Exhibit A-3: "Emerald - Conceptual Overview" and the additional references listed on pages 1-2 of Exhibit A-3;

- Exhibit A-4: "Emerald - Conceptual Design 1997" and the additional references listed on pages 1-2 of Exhibit A-4;

- Exhibit A-5: "Emerald - Live Traffic Analysis" and the additional references listed on page 1 of Exhibit A-5;

- Exhibit A-6: "Network NIDES" and the additional references listed on page 1 of Exhibit A-6;

- Exhibit A-7: "Ji-Nao" (includes "Ji-Nao" and "Ji-Nao slides") and the additional references listed on page 1 of Exhibit A-7;

- Exhibit A-8: "NSM" and the additional references listed on page 1 of Exhibit A-8;

- Exhibit A-9: "DIDS February 1991 and DIDS October 1991" and the additional references listed on pages 1-2 of Exhibit A-9;

- Exhibit A-10: "GrIDS 1996 and GrIDS 1997" and the additional references listed on page 1 of Exhibit A-10;

- Exhibit A-11: "NetRanger" (includes "NetRanger User Guide 1.3.1" and "NetRanger product") and the additional references listed on pages 1-2 of Exhibit A-11;

- Exhibit A-12: "RealSecure" and the additional references listed on page 1 of Exhibit A-12;

- Exhibit A-13: "Network Level Intrusion Detection;"

- Exhibit A-14: "U.S. Pat. No. 5,825,750" and the additional reference listed on page 1 of Exhibit A-14;

- Exhibit A-15: "Fault Detection in an Ethernet Network via anomaly detectors" and the additional references listed on page 1 of Exhibit A-15;

273698_1                                              8

- Exhibit A-16: "Stake Out Network Surveillance" and the additional reference listed on page 1 of Exhibit A-16;

- Exhibit A-17: "HP OpenView" and the additional references listed on pages 1-2 of Exhibit A-17;

- Exhibit A-18: "ISM" and the additional reference listed on page 1 of Exhibit A-18;

- Exhibit A-19: "Emerald 1997, Intrusive Activity 1991, NIDES 1994;"

- Exhibit A-20: Netstalker and HP OpenView" and the additional references listed on page 2 of Exhibit A-20;

- Exhibit A-21: "Network Flight Recorder" and the additional references listed on pages 1-2 of Exhibit A-21; AND

- Exhibit A-22: "AIS."

Citations to particular pages of a prior art reference in the attached prior art charts are to be understood as exemplary. Other pages of a prior art reference may also be relevant to the existence of a claim element, and Symantec reserves its right to supplement the page citations provided, if necessary. Symantec further reserves the right to supplement its § 102 contentions with additional prior art references because Symantec's investigation is still preliminary.

### PRIOR ART REFERENCES THAT RENDER THE
### CLAIMS-AT-ISSUE OBVIOUS

In addition to anticipating the claims- at-issue, a very large number of combinations of the prior art references identified render some or all of the claims–at–issue obvious under 35 U.S.C. § 103. Representative examples of invalidating combinations of the prior art references are identified below. Symantec reserves the right to establish that any alleged "invention" claimed in the patents-in-suit would have been obvious and thus invalid under 35 U.S.C. § 103 based upon any combination of references identified herein, or similar to those identified herein, that one skilled in the art as of Nov. 9, 1998 would have had motivation to create.

- Exhibit A-2: "Emerald - CMAD" (for indicated claims);

- Exhibit A-3: "Emerald - Conceptual Overview" (for indicated claims);

- Exhibit A-4: "Emerald – Conceptual Design 1997" (for indicated claims);
- Exhibit A-17: "HP OpenView" (see page 2 of Exhibit A-17 regarding § 103 combinations);
- Exhibit A-18: "ISM" (see page 1 of Exhibit A-18 regarding § 103 combinations);
- Exhibit A-19: "Emerald 1997, Intrusive Activity 1991, NIDES 1994" (see page 1 of Exhibit A-19 regarding § 103 combinations);
- Exhibit A-20: "NetStalker and HP OpenView" (see page 2 of Exhibit A-20 regarding § 103 combinations);
- Exhibit A-21: "Network Flight Recorder" (for indicated claims);
- Exhibit A-23: Summary chart of other relevant prior art, listing, for each individual limitation of each claim-at-issue, the prior art references that satisfy each limitation and could be combined with any of the references listed in Exhibits A-1 – A-22.

Symantec has provided as Exhibit A-23 a chart indicating prior art references disclosing particular limitations of each claim-at-issue. Given the large number of combinations, Symantec cannot identify all of the possible permutations at this time. For each of the prior art charts listed above for anticipation and/or obviousness, any missing claims or limitations could be satisfied by combining the cited reference of the prior art chart with reference(s) from Exhibit A-23. Symantec reserves the right to combine the cited references in any combination or permutation that one of skill in the art as of Nov. 9, 1998 would have had motivation to create or evaluate. Symantec further reserves the right to supplement its § 103 contentions with additional prior art references because Symantec's investigation is still preliminary.

## THE CLAIMS-AT-ISSUE ARE INVALID PURSUANT TO 35 U.S.C. § 112

The claims-at-issue are also invalid for failure to satisfy the best mode requirement under 35 U.S.C. § 112. SRI submitted source code in an Appendix to the patents-in-suit. A preliminary examination of the source code provided in the Appendix indicates that the code in the Appendix is not the complete program that existed at the time. For example, the Appendix code would not compile and run. In addition, the Appendix code contains no configuration files

10

allowing for the use of any particular network traffic data categories. Furthermore, the Appendix

code does not appear to have code for a resolver or an expert system. On information and belief,

Symantec believes discovery will show that SRI had a more complete set of source code by the

time it filed U.S. Patent Application No. 09/188,739 and withheld much of that code from the

Patent Office. That withheld code reflected the inventors' best mode of practicing the claims-at-

issue.

    In addition, the patents-in-suit are invalid for failure to satisfy the enablement and written

description requirements of 35 U.S.C. § 112. Furthermore, the claims-at-issue are invalid as

indefinite because the claims fail to particularly point out and distinctly claim the subject matter

of the invention.

    Symantec's contentions regarding the invalidity of SRI's patents-in-suit pursuant to 35

U.S.C. § 112 are preliminary and subject to modification and review. For example, Symantec

has not yet had the opportunity to depose either of the inventors.

Dated: January 19, 2006

DAY CASEBEER
MADRID & BATCHELDER LLP

By: _Paul Grewal/HL_
           Paul S. Grewal

Paul S. Grewal (*pro hac vice*)
Day Casebeer Madrid & Batchelder LLP
20300 Stevens Creek Blvd., Suite 400
Cupertino, CA 95014
Tel: (408) 873-0110
Fax: (408) 873-0220

*Attorneys for Defendant and Counterclaim-*
*Plaintiff* Symantec Corporation

11

OF COUNSEL:

Lloyd R. Day, Jr. (*pro hac vice*)
Robert M. Galvin (*pro hac vice*)
Paul S. Grewal (*pro hac vice*)
Day Casebeer Madrid & Batchelder LLP
20300 Stevens Creek Blvd., Suite 400
Cupertino, CA  95014
Tel:  (408) 873-0110
Fax: (408) 873-0220

Michael J. Schallop (*pro hac vice*)
Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA  95014
Tel:  (408) 517-8000
Fax:  (408) 517-8121

Dated:  January 19, 2006

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC.,
a California corporation,

      Plaintiff and
      Counterclaim-Defendant,

   v.

INTERNET SECURITY SYSTEMS, INC.,
a Delaware corporation,
INTERNET SECURITY SYSTEMS, INC.,
a Georgia corporation, and
SYMANTEC CORPORATION,
a Delaware corporation,

      Defendants and
      Counterclaim-Plaintiffs.

Civil Action No. 04-1199 (SLR)

## CERTIFICATE OF SERVICE

274306-1

01/19/2006 17:32 FAX                                                                    ☑016/016

## CERTIFICATE OF SERVICE

I, Howard T. Loo, hereby certify that on January 19, 2006 a true and correct copy of:

**SYMANTEC CORPORATION'S FOURTH SUPPLEMENTAL RESPONSE TO SRI INTERNATIONAL, INC.'S INTERROGATORY NO. 6**

was caused to be served on counsel as indicated:

**VIA FEDERAL EXPRESS and FACSIMILE**

Timothy Devlin, Esq.
Fish & Richardson, P.C.
919 North Market Street, Suite 1100
Wilmington, DE 19801

Richard L. Horwitz, Esq.
David E. Moore, Esq.
Potter Anderson & Corroon LLP
Hercules Plaza, 6th Floor
1313 Market Street
Wilmington, DE 19801

Howard G. Pollack, Esq.
Gina M. Steele, Esq.
Fish & Richardson, P.C.
500 Arguello Street, Suite 500
Redwood City, CA 94063

Holmes Hawkins, III, Esq.
King & Spalding
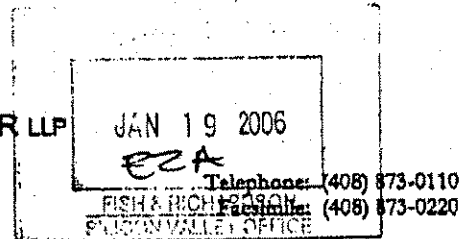191 Peachtree Street, N.E.
Atlanta, GA 30303-1763

_Howard Loo_
Howard T. Loo

274506-1                                          -2-

01/19/2006 17:30 FAX                                                    ☑001/016

## DAY CASEBEER
### MADRID & BATCHELDER LLP

JAN 19 2006

Telephone: (408) 873-0110
FISH & RICH...
Facsimile: (408) 873-0220
SUSON VALLEY OFFICE

20300 Stevens Creek Blvd., Suite 400
Cupertino, California 95014

# FACSIMILE TRANSMISSION

**DATE:  JANUARY 19, 2006**                        **NO. OF PAGES:  16**

## PLEASE DELIVER TO:

| |
|---|
| **TIMOTHY DEVLIN** |
| FISH & RICHARDSON PC |

**PHONE NO.**    (302) 652-5070        **FAX NO.**    (302) 652-0607

| |
|---|
| **HOWARD G. POLLACK** |
| FISH & RICHARDSON P.C. |

**PHONE NO.**    (650) 839-5070        **FAX NO.**    (650) 839-5071

| |
|---|
| **RICHARD L. HORWITZ** |
| POTTER, ANDERSON & CORROON, LLP |

**PHONE NO.**    (302) 984-6000        **FAX NO.**    (302) 658-1192

| |
|---|
| **HOLMES J. HAWKINS III** |
| KING & SPALDING |

**PHONE NO.**    (404) 572-4600        **FAX NO.**    (404) 572-5100

| |
|---|
| **THERESA MOEHLMAN** |
| KING & SPALDING LLP |

**PHONE NO.**    (212) 556-2100        **FAX NO.**    (212) 556-2222

01/19/2006 17:30 FAX                                                    002/016

# DAY CASEBEER
## MADRID & BATCHELDER LLP

### FACSIMILE TRANSMISSION
### PAGE 2

FROM:    PAUL S. GREWAL

CLIENT No. :    1904-001

MESSAGE:

EXHIBITS TO FOLLOW VIA FEDERAL EXPRESS.

ORIGINAL(S) WILL BE SENT BY FEDERAL EXPRESS